Testimony of

James M. Sullivan
Deputy Assistant Secretary for Services
International Trade Administration, U.S. Department of Commerce

Before the

U.S. Senate Committee on Commerce, Science, and Transportation

Hearing: "The Invalidation of the EU-US Privacy Shield and the Future of Transatlantic Data Flows"

December 9, 2020

---

1. INTRODUCTION

Good morning, Chairman Wicker, Ranking Member Cantwell, and distinguished Members of the Committee.

Thank you for the invitation to testify about the EU-U.S. Privacy Shield Framework and the recent *Schrems II* decision by the Court of Justice of the European Union. I am heartened by your bipartisanship on the importance of cross-border data flows and appreciate the Committee's active engagement on Privacy Shield in the five months since the Court's ruling.

As the Deputy Assistant Secretary for Services in the International Trade Administration, I oversee the Office of Digital Services Industries and the team responsible for U.S. Government administration and oversight of the Privacy Shield Framework. During the three-year period between July 2017 and July 2020, the Privacy Shield Team and I led three successful joint annual reviews of the functioning of the Framework with the European Commission and European data protection authorities, and facilitated a 125 percent increase in the number of Privacy Shield participants—from 2,400 to 5,400 U.S. companies that relied on the Framework to conduct transatlantic trade.

The International Trade Administration's Office of Digital Services Industries has long been focused on digital trade and data governance issues, advocating for policies that support the free flow of data across borders as essential to global commerce. As such, I welcome this opportunity to comment on the status of transatlantic data flows today.

With the growth in Internet connectivity and accelerating digitization of the global economy, cross-border flows of data have become just as important to growing American jobs and global

competitiveness as U.S. trade in goods and services. Because the United States has been a preeminent innovator and early adopter of information and communications technology, our nation occupies a singular leadership role in the digital economy today.

With the July 16, 2020 decision by the Court of Justice of the European Union in the *Schrems II* case, however, data transfers from one of the United States' largest trading partners are now under serious threat. In addition to invalidating the European Commission's adequacy decision for the EU-U.S. Privacy Shield Framework, the *Schrems II* decision has also called into question the reliability of the other key mechanisms for moving personal data from Europe to the United States.

My testimony will first explore why transatlantic data flows are so important to the U.S. economy. I will then review briefly the differing regulatory approaches to data privacy in the United States and the European Union, and how we have managed to bridge those differences in the past through innovative frameworks like Privacy Shield. Finally, I will discuss the *Schrems II* decision, its implications for U.S. businesses, and the Administration's efforts to restore legal certainty around transatlantic data flows by negotiating mutually acceptable standards of data privacy through targeted enhancements to the Privacy Shield Framework.

At the outset, I should note that I am limited as to what details I can share at this time with respect to discussions with the European Commission.

2. IMPORTANCE OF TRANSATLANTIC DATA FLOWS

The ability to transfer data—including consumers' personal data—seamlessly across borders generates enormous benefits for our citizens, our businesses, and our nation.

It affords Americans greater opportunities and a better quality of life—by allowing us all to interact with people and organizations anywhere in the world and access an ever-growing number of goods and services that can be tailored to our individual needs and preferences.

It allows our businesses, no matter how large or small, to use the Internet to more easily market and deliver their ideas, goods and services—wherever data is allowed to flow. Today, solo entrepreneurs and small- and medium- sized enterprises can reach global markets—and the 4.5 billion people now connected to the Internet—with unprecedented ease. American businesses of all sizes in every industry rely on personal data to facilitate transactions; enhance efficiencies; reduce costs; generate new customer insights; improve the quality of products and services; prevent and mitigate fraud; and manage their international networks of employees, customers, and suppliers.

With technologies like 5G, the Internet of Things, robotics, and artificial intelligence, the next wave of digital innovation is already here, and the ability to transfer data across borders—to and from Europe and other places in the world—is an essential driver of commercial competitiveness, economic growth, innovation, job creation, and wage growth worldwide. The economic benefits are clear not only for the United States but for Europe itself. At this particular moment in history, moreover, international data flows enable the data sharing and collaborative research critical to understanding the COVID-19 virus, mitigating its spread, and expediting the discovery and development of treatments and vaccines.

The United States and the European Union enjoy a $7.1 trillion economic relationship—with $5.6 trillion in transatlantic trade annually. According to some estimates, nearly $450 billion of this trade involves digital services. In truth—given the ongoing digitization of virtually every industry sector and the fact that cross-border data flows between the U.S. and Europe are the highest in the world—far more of that overall $5.6 trillion in trade is facilitated in some way by cross-border transfers of data.

3. DIFFERENT APPROACHES TO DATA PRIVACY

Despite our shared recognition of the importance of consumer privacy and data protection, the United States and the European Union differ in our respective legal approaches.

As a general matter, the United States does not have one comprehensive data protection or privacy law. Privacy is regulated through a number of laws enacted at the federal and state level. Federal laws often vary considerably in their purpose and scope. Many federal laws impose data protection requirements tailored to specific sectors, such as finance, health, and communication. Several federal laws focus on protecting certain types of particularly sensitive and at-risk consumer data. These include an individual's financial and medical information; children's online information; background investigations and "consumer reports" for credit or employment purposes; and certain other specific categories of data. All 50 states have also enacted legislation requiring private or governmental entities to notify individuals of security breaches of personally identifiable information.

The European Union, by contrast, largely protects *all* personal data under a single set of rules set forth in one law—the General Data Protection Regulation or "GDPR."

As a general matter, EU law also prohibits a company from transferring EU personal data outside Europe except under special circumstances.

First, transfers are expressly permitted to a recipient in a third country if the European Commission has determined that the national laws of that country provide an "adequate level of

protection" for personal data which is "essentially equivalent" to the level afforded under EU law. There are only 12 jurisdictions in the entire world that the European Commission currently considers to ensure an adequate level of protection: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and Japan.

And second, if there is no adequacy decision for a country, a company may still transfer EU personal data to a recipient in that country by using an EU-approved "transfer mechanism" that ensures sufficient data protection by the recipient. Standard Contractual Clauses or "SCCs" are the main transfer mechanism used by 90 percent of companies that transfer EU personal data internationally. Another option, Binding Corporate Rules or BCRs, is a set of legally enforceable internal policies for data transfers *within* a group of enterprises, typically large multinational organizations. Owing to a lengthy and expensive approval process, however, relatively few organizations—only about a hundred around the world—have adopted BCRs.

As the European Commission has not made an adequacy decision for the United States as a whole, the primary EU-approved data transfer mechanisms used by U.S. companies have been SCCs and, until recently, the EU-U.S. Privacy Shield, which was a "partial" adequacy decision in that it only covered transfers to Privacy Shield-certified companies in the United States.

The EU-U.S. Privacy Shield Framework

Privacy Shield was negotiated as a successor to the 15-year old Safe Harbor Framework. Under Safe Harbor, over 4,000 U.S. companies made legally enforceable promises that allowed for the transfer of EU personal data to the United States in compliance with EU law. In 2013, Austrian data privacy activist Max Schrems challenged Safe Harbor, and in 2015—spurred by Edward Snowden's unauthorized disclosures of national security information—the Court of Justice of the European Union invalidated the European Commission's adequacy decision that had underpinned the Framework since 2000.

To address the *Schrems I* decision, and in anticipation of GDPR's implementation in 2018, the Department of Commerce and its interagency partners worked with the European Commission to develop and maintain a modernized and durable transatlantic data protection framework. After months of intense negotiations, the United States and the European Commission finalized the EU-U.S. Privacy Shield Framework in July 2016.

Under the terms of the new Framework, the United States created the Privacy Shield Ombudsperson Mechanism at the State Department to investigate certain requests from EU individuals related to national security access to EU personal data transmitted to the United States. Because the Privacy Shield Ombudsperson Mechanism applied to EU personal data transmitted to the United States pursuant to *any* transfer tool approved under EU law (including

SCCs and BCRs), Privacy Shield became a key enabler of *all* transfers of EU personal data to the United States.

The International Trade Administration's Privacy Shield Team serves as the interagency lead for the Framework and administers the day-to-day functioning of the Privacy Shield Program. It works with eligible organizations seeking to certify to the Framework by verifying that they have developed a Privacy Shield-compliant privacy policy; identified an independent recourse mechanism to investigate complaints; contributed to an arbitration fund; implemented compliance procedures; and designated a representative to handle questions, complaints, data access requests, and other issues related to the organization's participation in the Program.

Once the Privacy Shield Team finalizes an organization's certification, it then adds that organization to the public-facing "Privacy Shield List". This list enables European companies or other interested parties to verify whether data can be transferred to the organization under the Framework.

An organization's public commitments to abide by the Framework's requirements are legally enforceable. Accordingly, to support the integrity of the Program, the Privacy Shield Team monitors organizations' compliance and potential "red flags" on an ongoing basis—and refers matters that may warrant further investigation to the Federal Trade Commission or the Department of Transportation for potential enforcement action as necessary.

In addition, each year since 2017, senior U.S. and EU officials have convened to conduct intensive two-day reviews of the functioning of the Privacy Shield Program. As noted earlier, the Privacy Shield Team and I led three successful annual reviews of the Program together with the European Commission, European data protection authorities, and U.S. Government colleagues from the Departments of State, Justice, and Transportation, the Office of the Director of National Intelligence, the Federal Trade Commission, and the Privacy and Civil Liberties Oversight Board, among others.

Our regular interactions with EU officials before, during, and after these annual Privacy Shield reviews afforded numerous constructive opportunities for transatlantic coordination and cooperation on promoting trust in the digital economy. Following the third annual review in Washington, DC in October 2019, for example, European Commissioner for Justice Věra Jourová enthusiastically acclaimed Privacy Shield a "success story".

For four years, Privacy Shield was the most straightforward and cost-effective EU-approved transfer mechanism for U.S. and European companies of all sizes in virtually every industry. For many firms—and for small- and medium-sized firms especially—Privacy Shield was often the *only* viable data transfer mechanism. Many such firms simply do not have the resources or

administrative capacity to utilize more costly and burdensome mechanisms like SCCs or BCRs. Of the 5,400 Privacy Shield participants on July 16, 2020, over 70 percent were small- and medium- enterprises with fewer than 500 employees.

4. *SCHREMS II*

The July 16, 2020 *Schrems II* decision was the latest development in a long-running legal battle that has been waged in the Irish courts and the EU Court of Justice by Max Schrems. As framed by the Court, the central question in the case was whether—in view of U.S. law and practice regarding government access to personal data for national security purposes—Privacy Shield and SCCs provided sufficient safeguards to EU personal data transferred to the United States. Although the European Commission and several EU Member States joined the U.S. Government in arguing that U.S. law and practice *do* in fact satisfy EU data protection standards, the Court answered the question with respect to Privacy Shield with a definitive "no".

The Court based its decision on two principal grounds. First, after analyzing the European Commission's 2016 adequacy decision for Privacy Shield, it found that certain U.S. intelligence access to EU personal data transferred under the Framework was not constrained in a way that satisfies the EU's legal requirement for "proportionality". Second, the Court concluded that the Privacy Shield Ombudsperson Mechanism did not afford sufficient redress for violations of EU individuals' right to data protection.

The *Schrems II* decision has created enormous uncertainties for U.S. companies and the transatlantic economy at a particularly precarious time. Immediately upon issuance of the ruling, the 5,400 Privacy Shield participants and their business partners in the EU could no longer rely on the Framework as a lawful basis for transferring personal data from Europe to the United States. Because neither the Court nor European data protection authorities provided for any enforcement grace period, Privacy Shield companies were left with three choices: (1) risk facing potentially huge fines (of up to 4 percent of total global turnover in the preceding year) for violating GDPR, (2) withdraw from the European market, or (3) switch right away to another more expensive data transfer mechanism.

Unfortunately, because of the Court's ruling in the Privacy Shield context that U.S. laws relating to government access to data do *not* confer adequate protections for EU personal data, the use of other mechanisms like SCCs and BCRs to transfer EU personal data to the United States is now in question as well.

Since the *Schrems II* decision, the lack of legal clarity regarding data transfers from Europe to the United States has prompted some companies to begin considering data localization in Europe. Storing and processing *all* EU personal data in Europe, however, would be exceedingly

expensive—especially for small- and medium-sized enterprises—and pose numerous technical problems for the global business models of most U.S. companies operating in Europe. Beyond the costs to individual firms, data localization measures can increase cybersecurity and other operational risks and make regulatory compliance and global risk management more difficult. Moreover, in our increasingly digitized economy, embracing data localization in Europe would set a damaging precedent for other countries and could imperil the open, interoperable, secure, and reliable Internet on which our citizens and businesses of all sizes have come to depend so heavily.

Suffice to say, the *Schrems II* ruling also calls into question the ability of European governments to share data with the United States for national security and law enforcement purposes, putting citizens on both sides of the Atlantic at risk. European authorities should recognize that the mere location of data does not ensure information security or privacy, and there are other public policy objectives that are equally important, including financial stability, operational resilience, and innovation – all objectives that depend on cross-border data flows.

U.S. Government Response to Schrems II

While we were deeply disappointed and do not agree with the Court's decision, we are committed to working with our European Commission partners to address the Court's concerns and enable companies to continue to transfer personal data from the EU to the United States. The Administration seeks to ensure the continuity of transatlantic data flows in a manner consistent with U.S. economic and national security interests.

It is important to note that the *Schrems II* ruling focused exclusively on government access to data. The Court did not question the extensive protections Privacy Shield offers EU individuals with respect to the commercial collection and uses of personal data. We believe Privacy Shield already provides strong and predictable protections for EU individuals and any enhancements to the Framework will build on this strong foundation.

As a first step in our efforts to return stability to transatlantic data flows, we engaged with the European Commission to begin working on a solution to Privacy Shield's invalidation. On August 10, Secretary Ross and European Commissioner for Justice Reynders released a joint statement announcing that the U.S. Department of Commerce and the European Commission had initiated discussions on potential enhancements to Privacy Shield Framework that address the Court's concerns.

Thereafter, in view of the considerable uncertainties concerning the use of SCCs, we worked with our interagency colleagues to bolster companies' ability to utilize the SCCs while we worked to negotiate the necessary enhancements to Privacy Shield. To that end the U.S.

Government released a White Paper to assist organizations using SCCs in making the case-by-case assessments called for under *Schrems II* as to whether U.S. law concerning government access to personal data meets EU standards. The White Paper includes a wide range of information about the extensive privacy protections in current U.S. law and practice relating to government access to data for national security purposes—and sets forth clearly the strong and multilayered protections provided under our system. While it is ultimately up to companies to make their own assessments under EU law, the White Paper has, by all accounts, proven to be a useful tool in conducting those assessments.

The objective of any potential agreement between the United States and the European Commission to address *Schrems II* is to restore the continuity of transatlantic data flows and the Framework's privacy protections by negotiating targeted enhancements to Privacy Shield that address the Court's concerns in *Schrems II*. Any such enhancements must respect the U.S. Government's security responsibilities to our citizens and allies.

To be clear, we expect that any enhancements to the Privacy Shield Framework would also cover transfers under all other EU-approved data transfer mechanisms like SCCs and BCRs as well.

The *Schrems II* decision has underscored the need for a broader discussion among likeminded democracies on the issue of government access to data. Especially as a result of the extensive U.S. surveillance reforms since 2015, the United States affords privacy protections relating to national security data access that are equivalent to or greater than those provided by many other democracies in Europe and elsewhere. To minimize future disruptions to data transfers, we have engaged with the European Union and other democratic nations in a multilateral discussion to develop principles based on common practices for addressing how best to reconcile law enforcement and national security needs for data with protection of individual rights.

It is our view that democracies *should* come together to articulate shared principles regarding government access to personal data—to help make clear the distinction between democratic societies that respect civil liberties and the rule of law and authoritarian governments that engage in the unbridled collection of personal data to surveil, manipulate, and control their citizens and other individuals without regard to personal privacy and human rights. Such principles would allow us to work with like-minded partners in preserving and promoting a free and open Internet enabled by the seamless flow of data.

5. CONCLUSION

In closing, the International Trade Administration, the Commerce Department, and the Administration remain committed to restoring clarity and certainty to transatlantic data flows and privacy as quickly as we can. We are hopeful that our European Commission partners share our

sense of urgency, and we appreciate the support and attention you and your colleagues here in Congress have brought—and can continue to bring—to the critical issue of cross-border data flows.

Thank you again for this opportunity to appear today.